Hacking new NFC cards

NTAG2x, Ultralight EV1/C, Desfire EV2, ISO-15693, meal EMV cards

abyssal • see #brmlab IRC for contact • 6.12.2018

New cards

- Mifare Ultralight C, Ultralight EV1
  - descendant of simple Ultralight
- meal card („stravenkova karta“)
  - essentially prepaid Mastercard EMV
- NTAG2x
  - a weird variant of Ultralight/Classic
- Desfire EV2
  - more features than EV1

Ultralight C/EV1

- old Ultralight just 64 bytes, C/EV1 more
  - 7 byte UID, locking
- Ultralight C
  - 3DES authentication, OTP, locking
- Ultralight EV1
  - 32bit password auth, OTP, anti-tearing
  - ECC signature of UID
  - version data, pack, read counters

Magic Ultralight C

```
      TYPE : MIFARE Ultralight C (MF0ULC) <magic>
       UID : 00 00 00 00 00 00 00
    UID[0] : 00, no tag-info available
      BCC0 : 00, crc should be 88
      BCC1 : 00, Ok
  Internal : 00, not default
      Lock : 00 00  - 0000000000000000
OneTimePad : 00 00 00 00  - 00000000000000000000000000000000

--- UL-C Configuration
 Higher Lockbits [40/0x28] : 00 00 00 00  - 0000000000000000
         Counter [41/0x29] : 00 00 00 00  - 0000000000000000
           Auth0 [42/0x2A] : 00 00 00 00  default
           Auth1 [43/0x2B] : 00 00 00 00  read and write access restricted
         deskey1 [44/0x2C] : 00 00 00 00  []
         deskey1 [45/0x2D] : 00 00 00 00  []
         deskey2 [46/0x2E] : 00 00 00 00  []
         deskey2 [47/0x2F] : 00 00 00 00  []

 3des key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Ultralight EV1 UID signature

```
--- Tag Information ---------
-------------------------------------------------------------
      TYPE : MIFARE Ultralight EV1 48bytes (MF0UL1101)
       UID : 04 0d d1 6a d0 4f 80
    UID[0] : 04, NXP Semiconductors Germany
      BCC0 : 50, Ok
      BCC1 : 75, Ok
  Internal : 48, default
      Lock : 00 00  - 0000000000000000
OneTimePad : 00 00 00 00  - 00000000000000000000000000000000

--- Tag Counters
       [0] : 00 00 00
                     - BD tearing Ok
       [1] : 00 00 00
                     - BD tearing Ok
       [2] : 00 00 00
                     - BD tearing Ok

--- Tag Signature
IC signature public key value :
04494e1a386d3d3cfe3dc10e5de68a499b1c202db5b132393e89ed19fe5be8bc61
    Elliptic curve parameters : secp128r1
            Tag ECC Signature : 3b be 8b a1 cc 1f 9e 2e 3e 8d 3f d6 4b e8 0b 99 f5 3b 9a 85
76 7f d5 d1 98 ac 75 94 81 d6 7f b1
```

ECC signature coincidence

- current brmdoor_libnfc has been designed with basically identical feature
  - I didn't know about NXP's design when I designed it for Desfire for brmdoor
  - prevents copy if you know just UID
- ECC signature over UID
  - different curves (NIST vs Ed25519)
- brmdoor uses Desfire's NDEF file, instead of special instruction (0x3C00)

NTAG1x, NTAG2x

- similar in features to Ultralight EV1
- few bytes storage (~144, depends on version)
- supports NDEF message, UID mirroring (NDEF URL with UID, e.g. http://as.df/UID)
- version, ECC signature (NIST-P256), OTP
- 32bit password
- everything sniffable ⇒ cloneable

Magic NTAG21x

- supports emulation of Ultralight EV1, various NTAG versions, „unbrickable“
- all features except EV1's anti-tearing
- everything except password can be sniffed from card
- password must be sniffed between reader and card
- 1-2 cm distance from Proxmark antenna required! Otherwise it will fail randomly

Ultralight EV1 clone on NTAG2x

```
pm3 --> hf mfu dump k ffffffff                    #dump EV1 with key FFFFFFFF on old card
pm3 --> script run mfu_magic -t 1                 #set type to Ultralight EV1 48 on Magic NTAG
pm3 --> hf mfu res f 0443D16AD04F80.bin s e r     #restore dump on Magic NTAG with magic commands
pm3 --> hf mfu info                               #see the result, you can „hf mfu dump" it as well
--- Tag Information ---------
-------------------------------------------------------------
      TYPE : MIFARE Ultralight EV1 48bytes (MF0UL1101)
       UID : 04 43 D1 6A D0 4F 80
    UID[0] : 04, NXP Semiconductors Germany
      BCC0 : 1E, Ok
      BCC1 : 75, Ok
  Internal : 48, default
      Lock : 00 00  - 00
OneTimePad : 00 00 00 00  - 0000
--- Tag Counters
       [0] : BF 08 6B
                    - 00 tearing failure
[...]
--- Tag Signature
IC signature public key name  : NXP NTAG21x (2013)
IC signature public key value : 04 49 4E 1A 38 6D 3D 3C FE 3D C1 0E 5D E6 8A 49 9B 1C 20 2D B5 B1 32 39
3E 89 ED 19 FE 5B E8 BC 61
    Elliptic curve parameters : secp128r1
            Tag ECC Signature : 88 6B 31 83 F8 3E C2 B3 9F 88 1F C5 15 F7 08 32 0F 9B 97 54 8E [...]
```

Desfire EV2

- extension of Desfire EV1
- all of EV1's features – applications & files
  - standard, backup, linear, cyclic, value, transaction MAC files
- mutual authentication DES/3DES/AES
  - key not sniffable
- EV2 proximity check, how does it work?
  - nothing in specs, I guess it's timing limit

Meal card (stravenkova karta)

- technically it's prepaid Mastercard EMV
- in Application Usage Control it allows usage in ATM
  - however backend will abort transaction
- 100% sure it would work on offline terminals
- approves any amount, not just 500 CZK
- a bit different CDOL1 (payment instruction data) from other Mastercards

Meal card payment request

```
opensc-tool -s '00 a4 04 00 0e 32 50 41 59 2e 53 59 53 2e 44 44 46 30 31 00' -s '00 a4 04 00
07 a0 00 00 00 04 10 10 00' -s '80 a8 00 00 02 83 00 00' -s '00 b2 01 14 00' -s '00 b2 01 1c
00' -s '00 b2 01 24 00' -s
'00 b2 02 24 00' -s '80 ae 50 00 42 00 00 00 00 50 00 00 00 00 00 00 00 02 03 00 00 00 00 00
02 03 14 03 14 00 cb 6d 9a 2c 22 00 00 00 00 00 00 00 00 00 00 1f 03 00 21 58 59 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00'

# Example of CDOL1 data for the EXECUTE:
 6 bytes - Amount, Authorized (9F02)             00  00  00  00  50  00  (50.0)
 6 bytes - Amount, Other (9F03)                  00  00  00  00  00  00
 2 bytes - Terminal Country Code (9F 1A)         02  03
 5 bytes - Terminal Verification Result (95)     00  00  00  00  00
 2 bytes - Transaction Currency Code (5F2A)      02  03
 3 bytes - Transaction Date (9A)                 14  03  14
 1 byte  - Transaction Type (9C)                 00
 4 bytes - Unpredictable Number (9F37)           cb  6d  9a  2c
 1 byte  - Terminal Type (9F35)                  22
 2 bytes - Data Authentication Code (9F45)       00  00
 8 bytes - ICC Dynamic Number (9F4C)             00  00  00  00  00  00  00  00
 3 bytes - Cardholder Verification Method (CVM) results (9f 34)      1f  03  00
 3 bytes - Transaction Time (9F 21)              21 58 59 (HH:MM:SS - in BCD?)
20 bytes - TLV (Context Specific)                00 00 ... 00 (20 zero bytes)
```

ISO-15693 changeable UID

- ski pass cards usually
- „vicinity“ vs „proximity cards“
  - up to 1.5 m in specs, practically ~50 cm
  - frequency as ISO-14443 (13.56 MHz)
- extremely simple
  - just UID, few bytes in few sectors (~320)
- newer versions claim to have AES auth, password, ECC signature of UID

Thanks

abyssal